Medical Identity Theft Environmental Scan

Contract Number HHSP233200045008XI

October 15, 2008

Prepared by:
Booz Allen Hamilton
One Preserve Parkway
Rockville, MD 20852
TEL: (301) 838-3600
FAX: (301) 838-3606

Prepared for:
United States Department of Health and Human Services
Office of the National Coordinator for Health Information Technology

Booz | Allen | Hamilton

TABLE OF CONTENTS

1.0 BACKGROUND

On April 27, 2004, President George W. Bush issued Executive Order 13335, which called for the development and nationwide implementation of an interoperable health information technology (health IT) infrastructure to improve the quality and efficiency of health care. This Executive Order established within the U.S. Department of Health and Human Services (HHS) the Office of the National Coordinator for Health Information Technology (ONC). The President outlined a plan to ensure that most Americans will have electronic health records (EHR)[1] by 2014. The use and implementation of health IT—such as EHRs, electronic prescribing, personal health records (PHR),[2] clinical decision support (CDS) tools, and secure electronic exchange of health information—is essential to the vision of a health care system that puts the needs and the values of the patient first and provides patients the information they need to make informed clinical and economic decisions in consultation with dedicated health care professionals.[3]

2.0 INTRODUCTION

For the purpose of this environmental scan, medical identity theft refers to the misuse of an individual's personally identifiable information (PII)[5] such as name, date of birth, social security number (SSN), or insurance policy number to obtain or bill for medical services or medical goods. Section 3.2 further explains the medical identity theft definition. Medical identity theft may result in the loss of accuracy in medical records; expenses to individuals whose identities are stolen; loss of trust by consumers for providers, insurers, and other health care stakeholders; and potentially, compromised patient care if inaccurate health records are relied on at the point of care.

The issue of medical identity theft is directly related to those sections in the Executive Order that refer to ensuring the secure transmission and protection of individually

Executive Order 13335: Incentives for the Use of Information Technology and Establishing the Position of the National Health Information Technology Coordinator—April 27, 2004

EO 13335 states that "[i]n fulfilling its responsibilities, the work of the National Coordinator shall be consistent with a vision of developing a nationwide interoperable health information technology infrastructure that:

Sec 2 (b): Improves health care quality, reduces medical errors, and advances the delivery of appropriate, evidence-based medical care.

Sec 2 (f): Ensures the patients' individually identifiable health information is secure and protected.[4]

1 An EHR is "a longitudinal electronic record of patient health information generated in one or more encounters in any care delivery setting. This information may include patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory information and radiology reports." ONC Emergency Responder Electronic Health Record (ER-EHR) Detailed Use Case, December 20, 2006. Available at <http://www.hhs.gov/healthit/usecases/documents/EmergencyRespEHRUseCase.pdf>

2 A PHR is "a health record that can be created, reviewed, annotated, and maintained by the patient or the care giver for a patient. The health record may include any aspect(s) of their health condition, medications, medical problems, allergies, vaccination history, visit history, or communications with their health care providers." Ibid.

3 Institute of Medicine (IOM). *Crossing the Quality Chasm.* The National Academies Press, March 1, 2001, p. 15.

4 Office of the Press Secretary, "Executive Order: Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator." April 27, 2004. <http://www.whitehouse.gov/news/releases/2004/04/20040427-4.html>.

5 The most broadly-applicable definition of Personally Identifiable Information (PII)is given by the Office of Management and Budget (OMB), which has defined PII as "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual." OMB Memorandum 06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006.

identifiable health information and a relevant consideration in the facilitation and development of a nationwide implementation of an interoperable health IT infrastructure to improve the quality and efficiency of health care. It is therefore important to explore the topic of medical identity theft and determine what effect it has on the security and protection of patients' health information in the context of electronic exchange.[6]

The President has dedicated considerable resources to investigating identity theft in general. In 2006, President Bush issued another Executive Order calling for a coordinated approach among government agencies to vigorously combat identity theft, and commissioned an Identity Theft Task Force to craft a strategic plan to make the federal government's efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution. The President's Task Force on Identity Theft issued its Strategic Plan on April 11, 2007, and found that "identity theft exacts a heavy financial and emotional toll from its victims, and it severely burdens our economy."[8]

Excerpt from the Presidential Identity Theft Taskforce Strategic Plan:

"The views [the President] you expressed in the Executive Order are widely shared. There is a consensus that identity theft's damage is widespread, that it targets all demographic groups, that it harms both consumers and businesses, and that its effects can range far beyond financial harm. We were pleased to learn that many federal departments and agencies, private businesses, and universities are trying to create a culture of security, although some have been faster than others to construct systems to protect personal information."[7]

3.0 PURPOSE

The broad purpose of this environmental scan is to serve as a baseline of knowledge and understanding for stakeholders regarding medical identity theft. Medical identity theft should be better understood and addressed for several important reasons. First, it can have a direct and devastating impact on consumers, health care providers, and other stakeholders in the health care system. Second, medical identity theft can damage the reliability, accuracy, and efficiency of health information exchange. These concerns may increase dramatically in an environment of electronic health exchange. Where medical identity theft results in the corruption of health information, a large electronic network can disseminate that corrupted information quickly and broadly. Moreover, if these networks do not have adequate privacy and security protections, large volumes of health information could be inappropriately accessed and used for, among other purposes, conducting medical identity theft.

The advantages that the electronic exchange of health information present over the current record-keeping system could be diminished if medical identity theft increases health care costs or if false health information is promulgated throughout the entire health care system, which could render patients' health records unreliable. However, health IT and health information exchange

---

6 Health Information, as defined by the HIPAA Privacy and Security Rules, is "[a]ny information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. 45 Code of Federal Regulation (CFR) Sec. 160.103.

7 Excerpt from the Presidential Identity Theft Task Force: Strategic Plan—Letter to the President, http://www.idtheft.gov/reports/StrategicPlan.pdf.

8 President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan." April 11, 2007 (p. viii).

could be used to prevent and detect medical identity theft in a manner that has not been previously available. In response to these concerns and opportunities, we conducted baseline research to understand more fully the scope and effects of medical identity theft.

Specifically, the purpose of the environmental scan is to develop an understanding of medical identity theft by—

- Identifying and compiling a list of organizations that have studied medical identify theft and summarizing their activities, as well as identifying the categories of stakeholders that may be significantly affected by medical identity theft
- Cataloging measures that have been discussed, are being established, or already exist to quantify medical identity theft and identify gaps where no reliable measures exist
- Identifying issues, focus areas, and activities underway to prevent, detect, and remediate medical identity theft and related issues, especially those that are relevant to the use, development, and implementation of health IT.

3.1 METHODOLOGY

Our approach consisted of conducting a literature review and stakeholder interviews, and participating in conferences that were specifically focused on medical identity theft. It became apparent that general information as well as data specific to medical identity theft was limited. As a result of our early review and based on stakeholder input, we determined that we needed to be aware of and consider medical identity theft in the broader context of identity theft as a whole. Therefore, we considered identity theft issues in the course of our investigations. Specific activities included identifying existing or forthcoming publications dedicated to medical identity theft and reviewing journal and newspaper articles on the topic. We also reviewed the Strategic Plan of the President's Identity Theft Task Force, the Federal Trade Commission's (FTC) *2006 Identity Theft Survey Report*,[9] and other documents related to other forms of identity theft. Furthermore, we tracked emerging issues, trends, and news items on identity theft.

In conducting telephone interviews, we identified and prioritized a number of individuals and organizations that have some knowledge of, or experience with, medical identity theft. In addition, we identified multiple stakeholders from categories, including government investigators and regulators, health professional associations, consumer interest groups, advocates, academic researchers, health IT experts, insurance companies, health care information organizations (HIO)[10], and commercial vendors. In all, 34 interviews were conducted between June and September 2008. Table 3-1 summarizes the interviews that the stakeholder group conducted. Appendix A contains a more detailed list of interviewees.

Table 3-1. Stakeholder Groups Interviewed

Stakeholder Group	Number of Interviews Completed
Providers	5

[9] Specific objectives of the survey were to estimate the prevalence of identity theft victimization, measure the impacts of identity theft on victims, identify actions taken by victims, and explore measures that may help victims of future cases of identity theft. The study was conducted through telephone interviews using Random-Digit-Dialing (RDD) sampling methodology. A total of 4,917 interviews were conducted between March 27 and June 11, 2006. See Federal Trade Commission *2006 Identity Theft Survey Report*. November 2007.

[10] HIOs are "organizations that oversee and govern the exchange of health-related information among organizations according to nationally recognized standards." See Section 4.4 of this environmental scan for more details on HIOs.

Stakeholder Group	Number of Interviews Completed
Payers	2
Professional Associations	5
Health Information Organizations	4
Federal Agencies	7
Consumer Interest Groups	6
Vendors/Technical Experts	6

Interviewees were asked to—

- Comment on their experience with, and knowledge of, medical identity theft
- Share any insights into the scope of the problem of medical identity theft
- Describe any existing or proposed known, effective methods for the prevention, detection, and/or remediation of medical identity theft
- Describe how health IT could be used to prevent, detect, and remediate medical identity theft, and conversely, to note any risks of medical identity theft that health IT poses
- Recommend potential next steps for assessing the scope of the issue more accurately.

No survey or interview instrument was used. For each interview, the interviewees' discussions were tailored to their area of expertise on the topic.

In addition, we attended conferences and presentations held during the same timeframe as the information-gathering phase of this project. These sessions were sponsored by the Blue Cross Blue Shield Association (BCBSA),[11] the American Health Information Management Association (AHIMA),[12] the Harvard Privacy Symposium,[13] United States Internal Revenue Service (IRS),[14] and the American Health Law Association (AHLA).[15]

3.2 MEDICAL IDENTITY THEFT DEFINED

For purposes of this environmental scan, the following definition will be used:

> **Medical identity theft refers to the *misuse* of another individual's PII such as name, date of birth, SSN, or insurance policy number to obtain or bill for medical services or medical goods.**

Other definitions of both "medical identity theft" and "identity theft" are available.[16] This definition, however, addresses the particular scope and purposes of this environmental scan. Given the importance of setting the scope of this topic, the rationale for developing this definition is discussed in detail below.

The most significant distinction between this definition and some others is that under this definition, medical identity theft may occur *with or without* the identified individual's consent or

[11] Blue Cross and Blue Shield Companies, Forum on Medical Identity Theft (Washington, DC: June 19, 2008). Webcast available at http://www.bcbs.com/news/bluetvradio/medical-identity-theft-forum/.
[12] AHIMA, Medical Identity Theft: A Virtual Meeting (Live teleconference with streaming video: September 8, 2008).
[13] Annual Privacy Symposium at Harvard University (Cambridge, MA: August 18–21, 2008).
[14] Internal Revenue Service, Identity Protection Forum (Washington, DC: July 21 and 22, 2008).
[15] AHLA, Red Alert – Red Flag Rules May Apply to You (Live teleconference: October 1, 2008).
[16] This definition has been developed for the specific purpose of this environmental scan. It is not intended to be a legal document.

knowledge. Therefore, the definition uses the term "misuse" to denote these instances of consent. We have considered examples of consensual acts because our objective in this environmental scan is to consider all forms of medical identity theft that may result in an individual's health record becoming corrupted. As a result, inaccurate health information may affect the individual's future medical care, or even his or her ability to receive health insurance, because those who access the record may rely on inaccurate health information to make decisions about the person's care or benefits. In addition, the existence of inaccurate health information may have secondary consequences on efforts in the public health or research domains.

In an attempt to ensure consistency with current research, we reviewed several other definitions of "medical identity theft." The World Privacy Forum, a nonprofit public interest research group, defines medical identity theft as the event that occurs "when someone uses a person's name and sometimes other parts of their identity—such as insurance information—without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods."[17] The sole significant difference in the World Privacy Forum definition is the exclusion of consensual events. Similar to the World Privacy Forum, the FTC definition of identity theft—which is broad enough to include, but is not specific to, medical identity theft—excludes cases where the incident occurs with the knowledge and consent of the individual whose identity is used: "[i]dentity theft occurs when someone uses your personally identifying information [...], without your permission, to commit fraud or other crimes."[18] Of note, however, is that other definitions are silent on the issue of consent: the President's Identity Theft Task Force[19] defines identity theft as "fundamentally, the misuse of another individual's personal information to commit fraud."[20] This definition is consistent with the definition we are using for purposes of this environmental scan. Perhaps significantly, the Task Force prefaced its definition by noting that "[i]dentity theft is defined in many different ways," and omits a discussion of the consent issue, which implicitly acknowledges that this definition may be appropriate in some circumstances. Finally, two notable federal laws address the issue of identity theft. Both the Identity Theft and Assumption Deterrence Act of 1998[21] and the Identity Theft Penalty Enhancement Act of 2004[22], state that identity theft is committed by "[w]hoever...knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[23]

After evaluating these definitions, we decided to consider medical identity theft to include cases where an individual uses the credentials of another—with or without that individual's knowledge or consent. This definition allows the environmental scan to consider all cases that have the consequences that are relevant, in particular, to the management of health records and health information exchange. Consensual events, as well as nonconsensual events, raise concerns about

17 Dixon, Pam. "Medical Identity Theft: The Information Crime That Can Kill You." World Privacy Forum, May 3, 2006, p. 5.
18 See Federal Trade Commission, "Fighting Back Against Identity Theft: About Identity Theft."
19 President's Identity Task Force, The Identity Theft Task Force, co-chaired by the Attorney General and the FTC Chairman, was established by Executive Order of the President on May 10, 2006, and now comprises 17 federal agencies and departments.
20 See President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007, p.10.
21 See Public Law (PL) 105-318 (Incorporated at 18 USC Sec. 001).
22 See PL 108-275 (Incorporated at 18 USC Sec. 1028A).
23 Ibid.

data integrity and the privacy and security of health information, and are important for ensuring the effective electronic exchange of health information.

To further clarify the definition of medical identity theft for purposes of *this environmental scan*, the following scenarios were developed. These examples are illustrative, not exhaustive.

Scenario 1. A person (the "thief") uses the identity of another (the "victim") to obtain medical care because the thief is uninsured. The victim may or may not be aware of and consent to the thief's actions. This situation arose, for example, when a woman permitted her cousin to use her health insurance information so that she could receive insurance coverage for giving birth at a large academic medical center in Massachusetts. This misuse was not discovered until the woman was asked to provide information to complete the birth certificate, at which time she offered her true information.

Scenario 2. A thief uses the identity of another to obtain medical care because the thief does not want the health records to include information about his or her health status. The medical identity thief is motivated by the desire to prevent the thief's current employer, potential future employer, or insurance provider from knowing aspects of the thief's true health condition.

Scenario 3. A thief uses the identity of a victim to obtain a prescription for drugs with the intention of using them recreationally or selling them. The thief engages in this behavior for the purpose of obtaining drugs, although he or she has no clinical need for them and they provide no benefit to the thief's health.

Scenario 4. A thief obtains the health information of a victim. In a separate incident, the thief also steals the PII needed to pose as a physician and submits claims for reimbursement from an insurance provider for services never provided to any individual. Incidents following the fact pattern of Scenario 4 are not uncommon, and many can involve hundreds of identities and the submission of millions of dollars' worth of false claims. *Note that like Scenarios 1–3, the events in Scenario 4 expose the victims to the risks of having inaccurate information entered into their health records.*

An actual event similar to Scenario 4: Representatives from a ring of medical imaging companies approached individuals in California and offered them free transportation, food, and medical care medical tests. Technicians posing as physicians and other health care professionals asked these individuals to provide personal information and photocopies of their Medicare cards. In the course of delivering ultrasound and other medical imaging services, the thieves inserted false diagnoses into patients' medical files and submitted false claims to the state Medicare program. The amount of false claims to state Medicare programs ultimately exceeded $1 million. The thieves pled guilty to conspiracy to commit health care fraud.[24]

The following scenario does *not* meet the definition of medical identity theft being used in this environmental scan: A thief obtains access to a patient's billing records, including credit card and social security information, and uses that data fraudulently to obtain credit cards, credit accounts, loans, and commercial goods. Although this scenario takes place in a medical facility and may constitute "identity theft," it does not meet *this environmental scan's* definition of "medical identity theft." This type of identity theft is not

An actual event that does *not* meet the definition of medical identity theft: A Massachusetts Superior Court Judge sentenced a 55-year-old woman to 5 to 7 years in prison after the woman pleaded guilty to using credit information collected from medical records to purchase almost $100,000 in merchandise from various websites.[25]

[24] World Privacy Forum 2006 Report Reference 9: United States v. Dzugha, Case No. 5:05-cr-00589-JF, Indictment at 4-7 (N. Cal).

[25] Laczkoski, Michelle. "Hopedale woman sentenced in identity theft case" The Milford Daily News. August 20, 2008.

addressed in this environmental scan because it does not, by itself, pose any significant risk of introducing inaccurate health information into the victim's health record.

3.3 FREQUENCY AND IMPACT OF MEDICAL IDENTITY THEFT

In its 2006 Identity Theft survey, the FTC reported that 3 percent of all identity theft victims in the United States, or approximately 250,000 Americans, reported that their identity had been used fraudulently to obtain medical treatment, services, or supplies.[26] Although the medical identity theft issue has been discussed frequently in newspapers and other media channels, few studies aside from the FTC survey have made any attempt to quantify the scope of medical identity theft.[27] However, research on nonmedical identity theft, and on security and privacy breaches, may provide some insight.

From the interviews conducted, stakeholders' perceptions of the size of the risk of the medical identity theft problem vary widely. In an article in the *Chicago Tribune*, James Quiggle, Director of Communications for the Coalition Against Insurance Fraud, stated that medical identity theft "is the fastest-growing form of identity theft in America today."[28] Other stakeholders agree that medical identity theft is extensive and suspect that it will increase in parallel with rising health care costs and other economic factors. One IT specialist reported that after realizing that medical identity theft incidents were occurring at his hospital, he began tracking its frequency and identified several incidents each month over the span of 12 months. Many stakeholders believe that providers and consumers are not fully aware of the frequency of medical identity theft and the potential risks it poses. Others believe the problem is extremely rare and therefore does not warrant special attention. Further research will be necessary to obtain more reliable data and to determine the accuracy of these speculations.

Similarly, additional research is needed to determine the financial impact of medical identity theft. Research has been conducted, however, on the costs associated with breaches of records containing PII in general. While breaches do not always result in identity theft, research on the costs associated with responding to them may be helpful in beginning to quantify the costs incurred when a breach occurs that does result in identity theft. One such research study was The Ponemon Institute completed one such research study. This organization specializes in information and privacy management practices in business and government and is cited widely for its efforts to analyze and quantify privacy issues.[30] The Ponemon Institute's 2006 Annual Report suggests that when PII is inappropriately accessed as a result of "human error, technology problems, or malicious acts,"[31]

The burden of breaches to businesses is high.
Dr. Larry Ponemon, chairman and founder of the Ponemon Institute states, "the burdens companies must bear as a result of a data breach are significant. Tough laws and intense public scrutiny mean the consequences of poor data are steep and growing steeper for companies entrusted with managing stores of consumer data."[29]

[26] Federal Trade Commission, *2006 Identity Theft Survey*. Although this survey was based on consumer recollections and was not specifically designed to examine medical identity theft, it is one of the only attempts to measure the frequency of medical identity theft.

[27] The statistics from the FTC survey are based on a definition of identity theft that does not include consensual events. Section 3.2 explains the FTC definition of "identity theft."

[28] Graham, Judith. "Medical identity theft spreads." *Chicago Tribune*, August 26, 2008.

[29] *Ponemon 2006 Annual Report: Cost of a Data Breach.* "Understanding Financial Impact, Customer Turnover, and Preventative Solution," October 2006. Sponsored by PGP Corporation and Vontu. This study looked at 31 different companies across 15 industries that suffered data breaches ranging from 230,000 to 815,000 records.

organizations incur approximately $182.00 in expenses for each record that has been compromised and requires review and correction.[32] While this figure is not specific to incidents involving the compromise of health information, the activities required to correct corrupted health records may be comparable.

The effects of medical identity theft on the victim can range from general inconvenience to significant disruption to the victim's livelihood. The theft could, for example, result in the exhaustion of the victim's insurance benefits, and the victim may experience difficulties or delays in receiving future health care services or denial of coverage because of "pre-existing conditions" of the thief. The victim may be billed for deductibles, co-payments, or other costs of the health care delivered to the thief. Victims may receive calls from collections agencies retained by health care providers. Victims can be burdened with proving they are not responsible for these charges, and if they cannot, records of these unpaid costs can affect their credit rating. Furthermore, because health information often flows to different recipients, such as primary care providers, specialists, health care business associates, insurance plans, researchers, and others, the corruption of patient information can have what the AHIMA refers to as a "cascading effect." As health information is provided to different users, each user, as well as the victim, can experience distinct and negative effects.[33] The most dangerous consequence for the victim occurs when incorrect health information enters the patient's health record. If a provider relies on false health information, he or she could provide inappropriate care, such as transfusing the wrong blood type, performing procedures that are unnecessary or even harmful, or prescribing inappropriate medications that could cause an adverse drug interaction.

4.0 MEDICAL IDENTITY THEFT STAKEHOLDERS

It is important to raise awareness of medical identity theft and the associated ramifications to properly understand how health information management professionals and others can work together to prevent, detect, and remediate the damage and impact it may cause to various stakeholders. The primary victim of medical identity theft is the consumer,[34] but other stakeholders include payers, providers, HIOs, federal agencies, and commercial vendors. In this section, the effects of medical identity theft on each of these groups are considered, as well as each group's potential role in responding to the issue.

4.1 CONSUMERS

For purposes of this environmental scan, "consumers" either are patients who receive medical attention, treatment, or care or are patients' family members or caregivers that pay for or are otherwise involved in patients' care. Consumers play a critical role in the basic health care information delivery chain because they communicate and provide their own health information to health care providers, payers, and other stakeholders in the system.

---

30 Ponemon Institute. The Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices in business and government. http://www.ponemon.org.

31 *Ponemon 2006 Annual Report: Cost of a Data Breach*. "Understanding Financial Impact, Customer Turnover, and Preventative Solutions," October 2006. Sponsored by PGP Corporation and Vontu. This study looked at 31 different companies across 15 industries that suffered data breaches ranging from 230,000 to 815,000 records.

32 Ibid.

33 Apgar, Chris et al. "Mitigating Medical Identity Theft." *Journal of AHIMA*, July 2008, p. 63–69.

34 AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79:7 (July 2008): 63–69.

Consumers are directly affected by medical identity theft. In cases where medical identity thieves have used consumers' health insurance information to receive health care, they may drain the consumers' coverage limits, incur co-payments, or otherwise create the appearance of a financial obligation. Even more significantly, however, in the course of receiving health treatment under another's identity, false health information may be introduced into consumers' health record, which can have consequences to the consumers' future health care, possibly including receiving inappropriate treatment. Consumers therefore have a significant interest in correcting their health records if they discover they have been the victims of medical identity theft. This discovery can require significant time and money and cause the consumer considerable frustration and stress.[35] If the appropriate corrections are not made, consumers may be burdened with damage to their credit rating, suffer loss or denial of health coverage, or endure increased health premiums. In fact, in at least one case, inaccurate health information created the appearance that the consumer was abusing drugs, and a state agency attempted to place her children in protective custody.[36]

Consumers themselves may be the best "first line of defense" against medical identity theft. In many cases, incorrect billing or diagnostic inconsistencies are generally reported first by the consumer, although some time may pass after the incident before the consumer becomes aware of it. Consumers may not know that they have been victims of medical identity theft until they receive suspicious or incorrect bills or until debt collectors contact them for late payments for fraudulent health services provided to a medical identity thief.

An Example of a Consumer Detecting Medical Identity Theft: In 2004, a Florida woman was billed for a surgical procedure she did not receive, which she believed was simply a billing error. When she was hospitalized a year later, however, her suspicions were raised when a nurse reviewing her chart commented on information in her record indicating she was diabetic. The woman knew this information was inaccurate and was ultimately able to demonstrate that her medical record had been corrupted.[37]

In cases like these, consumers are in the best position to identify discrepancies because they are the only ones that truly know what health services they received. Some stakeholders already recognize the critical role consumers play in preventing medical identity theft. One major payer, for example, conducts consumer education about medical identity theft and advises its beneficiaries to safeguard their insurance cards in the same way they would safeguard their credit cards.[38]

As the health care system increasingly relies on the electronic collection, storage, and transfer of health information, consumers will be able to select from a number of emerging technologies for managing their health information. PHRs,[39] for example, have become more readily available to consumers with the launch of many commercial offerings from both large and small software companies. A large health provider organization provides a PHR to more than 8.7 million patients, allowing them to email their doctors, view lab results, and schedule appointments.[40] Although consumers already have the right of access to their own health care records under the Health Insurance

35 Coalition Against Insurance Fraud. "Medical Identity Theft." http://www.insurancefraud.org/medical_id_theft.htm
36 "Protect Against Medical ID Theft: Medical ID Theft Nearly Ruined a Good Mother's Life" CBS News. October 9, 2006.
37 "Diagnosis: Identity Theft," *Business Week*, January 8, 2007.
38 Blue Resources, Anti-Fraud. "What You Can Do to Help Prevent Healthcare Fraud and Abuse." Blue Cross Blue Shield Association.
39 The National Alliance for Health Information Technology: Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms. April 28, 2008.
40 Dolan, Pamela Lewis. "Kaiser's PHR online for all members," *American Medical News*. November 26, 2007. http://www.ama-assn.org/amednews/2007/11/26/bise1126.htm

Portability and Accountability Act (HIPAA) Privacy Rule,[41] tools such as these allow them the ability to more readily detect medical identity theft because they are able to more easily view their records, identify errors, and recognize inconsistencies.

4.2 PAYERS

For purposes of this environmental scan, "payers" are entities that accept responsibility for payment to providers on behalf of enrolled consumers. They include organizations and institutions such as health insurance plans, federal programs, and health care sponsors, such as employers or unions. Health care payers and providers are attractive targets for both medical and financial identity thieves because they collect and maintain large quantities of health information. The data includes sensitive personal and financial information that can be used to steal a consumer's identity, to receive health care benefits, to submit false claims, or to sell to black marketers who can use the information for fraudulent purposes. In addition, health records are valuable targets because they are usually maintained in a central location that provides access to a large number of records, enabling thieves to carry out massive frauds. As the insurance industry migrates to an electronic claim submission environment, these records become more portable and are vulnerable to inappropriate access from anywhere in the world.[42]

Payers may suffer several types of financial consequences of medical identity theft. They may bear the costs of services provided in incidents of medical identity theft. The costs of these services are not offset by the receipt of premiums and can damage payers' ability to plan for, control, and manage overall costs. After a medical identity theft occurs, payers may incur significant expenses working with victims to remediate fraudulent activity. They may also incur costs in addressing the privacy and security weaknesses exploited to conduct medical identity theft. Finally, it is possible to incur negative publicity, which could affect their reputations and goodwill, resulting in lost business.

Payers may have an advantage in preventing and detecting medical identity theft. They have access to a large amount of health transaction data and may be able to conduct risk analyses that will identify trends and patterns that indicate medical identity theft or other forms of fraud. Conducting these analyses, however, can be a huge task that involves a significant overhead expense. Payers may therefore elect to conduct limited auditing activities, for example, by analyzing subsets of transaction data. Payers can also provide education and awareness to participating providers and consumers. This education increases the likelihood that these stakeholders will detect and report medical identity theft and may improve their legal standing and recourse to pursue financial recovery for medical identity theft.

[41] Under the HIPAA Privacy Rule, individuals have the right to "access to inspect and obtain a copy of protected health information about the individual in a designated record set," subject to some conditions and exemptions. See HIPAA Privacy Rule, 42 CFR § 164.524. Patients further have the right "to have a covered entity amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set," again, subject to some conditions and exemptions. See HIPAA Privacy Rule, 42 CFR § 164.526. Many PHRs, however, allow consumers to access their health care records electronically and allow instantaneous access without delays associated with making formal requests to individual providers.

[42] American Health Insurance Plans: Newsroom, March/April 2004. New industry regulations for transmitting claims information electronically.

4.3 PROVIDERS

Health care providers are those that provide health services to consumers. They may include physicians and other health care providers; hospitals; skilled nursing homes; long-term care and other facilities; and pharmacies, laboratories, and diagnostic facilities reporting test results.[44] Health care providers must maintain and protect sensitive patient information.[45] They also are responsible for providing the appropriate services and submitting claims to payers in accordance with governing laws.[46]

Identity Theft of a Provider:

A New York man was convicted of stealing $248,000 from Medicaid in 1987 by billing it under the name of a doctor who had interviewed him for a job in a one-room medical office. The man, who is not a doctor, was sentenced to 1 year in jail.[43]

Medical identity theft affects providers in two main ways. First, providers who rely on corrupted health records may provide inappropriate care, compromising patient health safety. Providers may have to defend their decisions based on services rendered from relying on a corrupted record that results in an adverse event. AHIMA notes that common law has not yet defined when actions a provider takes in the face of medical identity theft constitute negligence or malpractice, entitling the victim to receive compensation or take other legal action.[47]

Second, providers face a number of financial risks dealing with medical identity theft. A provider that incorrectly bills the victims of identity theft is at risk of writing off all expenses related to the services rendered.[48] Providers may incur additional administrative costs in identifying false claims and working with payers to address them. Additional overhead may be associated with identifying third parties that have received inaccurate health records and with ensuring victims' records are corrected to avoid future problems.

Health care providers can be affected in cases where their identities are stolen as part of the medical identity theft. In these instances, an unqualified individual steals the identity of the provider to submit false claims to a payer. Providers' reputations may be affected adversely if their identities were wrongfully used, and they may need to defend themselves against accusations of criminal behavior.

Providers may be able to take action to detect, prevent, and respond to medical identity theft incidents, but no single solution applies to all providers because each is unique in its size, overhead, and available resources. Various techniques that may be used, however, include conducting patient authentication, training and awareness, and risk assessments.

---

43 Associated Press. "Man Using Doctor's Identity Sentenced in Medicaid Fraud." *New York Times*.

44 "Defining Key Health Information Technology Terms." *The National Alliance for Health Information Technology.* April 28, 2008.

45 Lapidus, Brian. "TECH: Identity Theft Protection for Healthcare Companies" *The Health Care Blog.* August 9, 2007.

46 New Perspectives on Healthcare Risk Management, Control, and Governance. "Medical Identity Theft Protecting Patient Information Accounts Payable Fraud." Journal of the Association of Healthcare Internal Auditors. 26:3. (2007). Pg. 50.

47 AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79:7 (July 2008): 63–69.

48 AHIMA e-HIM Work Group on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79:7 (July 2008): 63–69.

4.4 HEALTH INFORMATION ORGANIZATIONS

Health Information Organizations are "organizations that oversee and govern the exchange of health-related information among organizations according to nationally recognized standards."[50] The role of the HIO is one of governance and oversight. The primary functions that most HIOs provide fall into categories of technical operations for the movement of information, accountability for regulatory and standards associated with information exchange, data sharing agreements, and facilitation of lessons learned among its participants. Regional Health Information Organizations (RHIO) are an example of a type of HIO "that brings together health care stakeholders within a defined geographic region and governs health information exchange among them."[51] Health data banks, specialty care organizations, and integrated delivery networks are other types of health information organizations.

Increasing health information exchange activity: In a 2007 survey of health information exchanges, 34 percent reported that they are exchanging laboratory data, and 32 percent are exchanging outpatient care data, up from 26 percent and 21 percent, respectively. In each of three other categories (emergency department, outpatient laboratory, and radiology results), at least 25 percent of respondents reported exchanging data as well. These results also represented increases over 2006 data.[49]

HIOs are affected by medical identity theft as it relates to their responsibility for the privacy and security of the health information they oversee. Depending on the nature and purpose of the organization, the type of health information HIOs oversee may include claims data, clinical results, patient medication, chronic disease histories, and other types of health information specific to individuals. The information requires proper handling not only in accordance with regulations such as HIPAA but also in a manner that will ensure confidence with participants that it will not be at risk of being breached.

Medical identity theft therefore has direct consequences for HIOs. Breaches that affect the organization, its participants, or third parties with whom HIOs exchange data may allow an internal or external party unauthorized access to the health information to commit medical identity theft.

HIOs may have problems responding to medical identity theft and other health IT breaches in a coordinated way because policies and practices at component organizations may differ. Based on our research, a limited number of standards are broadly or universally adopted across the health care industry for reporting and notifying affected entities in the event of medical identity theft. Furthermore, opinion varies on what threshold needs to be reached before notifying consumers of a breach that may lead to medical identity theft. Some HIOs believe that notification is needed whenever sensitive data is accessed without authorization, while others believe notification is needed only if the stolen data can be used to commit identity theft.[52] When developing an

[49] Ibid.
[50] The National Alliance for Health Information Technology: Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms. April 28, 2008.
[51] Ibid.
[52] "While there appears to be growing industry consensus that security breach notification laws have forced companies to take more responsibility for the data they own, there is little agreement on exactly when companies should be required to notify consumers when a data breach occurs. Ranged on one side of the debate are those who want alerts for any breach involving the potential exposure of sensitive data. On the other side are those who say that a higher disclosure threshold is needed to avoid over-notification and needless costs." Jaikumar Vijayan, Breach notification laws: When should companies tell all?,

approach, HIOs also are mindful that excessive breach notification can overwhelm consumers and lead to unnecessary costs and burden to stakeholders, including the HIOs themselves, consumers, health care providers, and payers. Developing policies for responding to medical identity theft may require internal policy development, training, implementation, and assurance that participants are responding consistently and in a coordinated way.

4.5 FEDERAL AGENCIES

Federal agencies conduct activities in many of the roles discussed in this environmental scan. Some, like Centers for Medicare and Medicaid Services (CMS), Indian Health Services, and the Veterans Administration (VA), are payers or providers of health care. Others, like the FTC, HHS Office of the Inspector General (OIG), or Department of Justice (DOJ), are law enforcement agencies that investigate and/or prosecute incidents of medical identity theft. Still others, like the Social Security Administration (SSA), may rely on records that may be corrupted as a side effect of an incident of medical identity theft. Finally, HHS's Office of Civil Rights (OCR) enforces the HIPAA Privacy Rule,[53] and CMS enforces the HIPAA Security Rule.[54] Enforcement of one or both may be appropriate if medical identity theft is a result of privacy and/or security practices that do not meet the requirements of these HIPAA rules.

Federal agencies are affected by medical identity theft in all of these capacities. DOJ, for example, conducts investigations and prosecutions of medical identity theft through its Health Care Fraud Section. In fiscal year 2007, through the cooperation of whistleblowers and the effective use of available resources, DOJ identified approximately 120 cases[55] of health care fraud that may meet the definition of "medical identity theft." As well as providing compensation and restitution for medical identity theft, DOJ also expects prosecution to serve as a deterrent to future incidents of medical identity theft. DOJ learns of these cases from several sources, including referrals from CMS, among others. OCR and CMS learn of privacy and security violations primarily through individual complaints. When it appears that the privacy or security incident is related to criminal activity, OCR and CMS refer these cases to DOJ for investigation and prosecution. CMS and OCR, however, also bear burdens related to investigating these claims if they indicate a breach of the HIPAA Privacy and/or Security rules.

Federal agencies may, in some cases, be able to obtain restitution for medical identity theft victims. For example, DOJ has had some success in obtaining these judgments when pursuing

Computerworld.com (March 2, 2006), available at http://www.computerworld.com/securitytopics/security/story/0,10801,109161,00.html

[53] The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule is the first comprehensive Federal protection for the privacy of personal health information. See http://www.hhs.gov/ocr/hipaa/privrulepd.pdf. All HIPAA-covered entities, including some federal agencies, must comply with the HIPAA Privacy Rule. See also Standards for Privacy of Individually Identifiable Health Information; Final Rule (The HIPAA Privacy Rule), 65 FR 82461, December 28, 2000.

[54] The Security Rule "specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. All HIPAA covered entities, which include some federal agencies, must comply with the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures." NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. See also Health Insurance Reform: Security Standards; Final Rule ("The HIPAA Security Rule"), 68 FR 8334, February 20, 2003.

[55] DOJ does not track cases by category of health care fraud. This figure is based on an estimation provided during a stakeholder interview.

financial identity theft cases through its Financial Litigation Unit. Restitution, however, may be limited or not available if defendants do not have the resources for compensation.

For federal agencies that are also payers, the cost of medical identify theft can be significant. According to the National Health Care Anti-Fraud Association, for example, approximately 3 percent of U.S. health care costs (roughly $60 billion) are fraud-related. The amount of this figure attributed to medical identity theft is not known, but even a small, single-digit percentage of this large figure amounts to a large sum.[56] Given that the federal government is the largest payer of health care costs in the United States, the financial impact of medical identity theft may be substantial. Other federal agencies bear costs related to medical identity theft as well, although these may be even more difficult to quantify. Federal enforcement agencies, for example, must bear the costs of pursuing these cases, which may require distinct costs related to specialized computer forensics or health care industry expertise.

Federal agencies' roles in responding to medical identity theft are as diverse as their relationships to it. Agencies that pay for health care, enforce the law, or set health care policy may need to invest in conducting research to measure medical identity theft's scope and effects. Federal agency payers also may need to develop pilot programs to determine the effectiveness of various controls in addressing medical identify theft, provide information and education to the public and stakeholder groups, and continue to identify it. Law enforcement agencies' roles are also critical in responding to the issue by investigating and prosecuting incidents.

4.6 COMMERCIAL VENDORS

Commercial vendors include providers of technical goods and services. During the course of conducting the environmental scan, vendors were consulted to determine what solutions already exist in the marketplace to address medical identity theft. Vendors offer a variety of products and services to manage activities. These services include auditing access of information systems, analyzing patterns of transactions, considering risk models to identify individuals at high risk for becoming victims of fraud, and monitoring use of individuals' information to detect inappropriate use.

Medical identity theft affects commercial vendors because it requires them to adjust the goods and services they provide to consider and address medical identity theft. While some products have emerged in response to the increasing prevalence of financial identity theft, the commercial entities included in this environmental scan now recognize the additional complexities posed by medical identity theft and are evaluating how their tools can be customized to account for its effects. Some commercial vendors are able to apply their knowledge, experience, and best practices from working with forms of identity theft other than medical identity theft as a starting point for developing medical identity theft products and services. One example is pattern recognition technology that currently may not be designed to specifically address medical identity theft but could be modified to do so. Commercial vendors also may be affected because if their current offerings do not anticipate medical identity theft, they may lose a market discriminator and competitive edge, or they may be liable if the effectiveness of their product is diminished.

[56] McKay, Jim. "Identity Theft Steals Millions from Government Health Programs." February 13, 2008.

Commercial vendors may have a role in responding to medical identity theft because they are able to identify the market needs it creates, and they are in a position to develop tailored or modified tools and solutions to help address it. Services that address health care fraud, identity theft, authentication, and records management may wish to consider the risk of medical identity theft in refining and updating their existing products. Finding effective (and cost-effective) ways of addressing this medical identity theft represents an opportunity for commercial entities.

5.0 CURRENT EFFORTS RELATED TO HEALTH IT PRIVACY AND SECURITY

The Department of Health and Human Services has the primary goal of "protecting the health of all Americans". Health IT is one of Secretary Leavitt's key priorities focused on improving health care quality, reducing costs and pursuing the benefits of interoperable health IT.[58]

Although the adoption of health IT is becoming more prevalent across the United States, it should be recognized that health IT has the potential for both positive and negative effects on medical identity theft. Electronic sharing of health information can enhance a provider's ability to have the right health information for the right patient at the point of care, which can inform decision making and identify an appropriate treatment plan. However, storing and transmitting large amounts of health information poses a significant risk in the event of a security breach.

Health IT presents potential advantages, but also potential risks. An Oregon-based medical center was named in July 2006 one of the nations "100 Most Wired Hospitals and Health Systems" and prides itself in using cutting-edge technology to improve patient care. However, in December 2006, a computer bag holding 10 computer disks containing medical data for 365,000 patients from the regional medical center was stolen from an employee's car. So far, no cases of identity theft associated with the breach have surfaced, but the center has spent $7 million responding to the error.[57]

A significant amount of work has been carried out by various stakeholders to research and analyze privacy and security issues that are unique to the sharing of health information. We reviewed the work of some groups whose findings are directly relevant to medical identity theft and health information exchange. Below is a summary of their most significant findings. While not all of these groups have called out medical identity theft as a discrete topic, all are conducting work on privacy and security that would have a direct effect on preventing, detecting, and remediating it.

Congress created the National Committee on Vital and Health Statistics (NCVHS) to advise HHS on issues related to health information, statistics, and national health information policy. The committee serves as a forum for the collaboration of interested parties to accelerate the evolution of public and private health information systems toward more uniform, shared data standards, operating within a framework protecting privacy and security.[59] Its work affects medical identity theft because it has endorsed expanding federal law related to preventing, detecting, and remediating privacy and security breaches, including medical identity theft. The subcommittee on privacy and security monitors major developments in health information privacy and confidentiality on behalf of the full committee, identifies issues and opportunities, makes recommendations to the full committee, and assists HHS in implementing the health

[57] Nichols, Cindy. *Medical Identity Theft.* American Health Information Management Association. Chicago. 2008. p 33-45.
[58] Secretary Mike Leavitt, U.S. Department of Health and Human Services. See http://www.hhs.gov/secretary/priorities/index.html
[59] National Committee on Vital and Health Statistics Charter. The Secretary of Health and Human Services. January 2008.

information privacy provisions.[60] In June 2007, the subcommittee delivered a letter that focused on updating privacy laws and regulations required to accommodate Nationwide Health Information Network (NHIN) data sharing practices. The subcommittee stated its belief that all entities handling individually identifiable health information should be covered by some federal privacy law.[61]

The *Health Information Security and Privacy Collaboration (HISPC)*, a federally funded project, was charged in 2006 to implement a national collaborative effort to address privacy and security policy questions affecting interoperable health information exchange.[62] Initially, 33 states and 1 territory participated, each looking to local stakeholders for input to ensure that proposed privacy and security solutions are consistent and representative of local needs. During this initial phase, the defined processes for each state were to (1) assess variations in organization-level business policies and state laws that affect health information exchange; (2) identify and propose practical solutions, while preserving the privacy and security requirements in applicable federal and state laws; and (3) develop detailed plans to implement solutions. Each participating state is focused on different "collaboratives" of security and privacy its aim to develop "common, replicable, multi-state solutions" that can then be applied nationally. HISPC is currently in phase 3 of its project, with now approximately 42 participating states that "comprise 7 multi-state collaborative privacy and security projects. Each project is designed to develop common, replicable multi-state solutions that have the potential to reduce variation in and harmonize privacy and security practices, policies, and laws." A cross-collaborative steering committee has been established for phase 3 to facilitate knowledge transfer among collaboratives and identify points of intersection.[63]

The *American Health Information Community (AHIC)*, a federal advisory committee created and chaired by the Secretary of HHS, established a Confidentiality, Privacy, and Security (CPS) workgroup with the specific charge of making recommendations to the community on policies that balance the protection of information with appropriate access to move the adoption of health IT forward.[64] The CPS workgroup produced specific recommendations regarding identity-proofing options for patients to gain access to their health information electronically. The implications for medical identity theft include that, if consumers have direct access to their medical records, they may be better able to detect medical identity theft and alert providers, payers, and other stakeholders to its occurrence, allowing faster and more efficient responses. AHIC accepted a number of these recommendations and forwarded them to the Healthcare Information Technology Standards Panel (HITSP) for consideration in developing interoperability specifications.

HITSP is a private sector body that is federally supported with the primary purpose of harmonizing and integrating standards for sharing clinical and business information. In 2007, HITSP began incorporating security and privacy standards into its interoperability specifications. HITSP developed Technical Note 900 and the underlying constructs to provide important

60 NCVHS Subcommittee on Privacy and Security. Charge. November 1996.
61 NCVHS Subcommittee on Privacy and Security. Letter to the Secretary. "Re: Update to Privacy Laws and Regulations required to accommodate NHIN data sharing practices." June 21, 2007.
62 Health Information Security and Privacy Collaboration (HISPC). RTI International. See http://www.rti.org/hispc
63 Health Information Security & Privacy Collaboration: Executive Summary. See http://privacysecurity.rti.org
64 http://www.hhs.gov/healthit/ahic/confidentiality.

guidelines on access controls, consent directives, and other security and privacy issues.[65] One effect of standardizing privacy and security constructs would be to enable the electronic exchange of health information, while minimizing vulnerabilities related to medical identity theft. In addition, the HITSP Security, Privacy, and Infrastructure technical committee formed a specific working group that focused on identity credentialing management. This group has done work related to identity credentials for activities such as user authentication and identity proofing. Strong user authentication will serve as a barrier to inappropriate access, including inappropriate access conducted for the purposes of perpetrating medical identity theft. The work from HITSP is incorporated into Certification Committee for Health Information Technology's (CCHIT) certification criteria.

CCHIT is a federally supported private sector body for EHRs, PHRs, and their networks.[66] In conjunction with its broader certification effort, CCHIT created a privacy and security expert panel to develop criteria for certifying systems and applications. These criteria mandate that certified systems support the designated standards regarding storage, authentication, encryption configuration, and other technical protocols developed and accepted by HITSP. EHRs that support these security standards may be less vulnerable to privacy and security breaches, including those that can ultimately lead to medical identity theft.

The *American National Standards Institute (ANSI),* a private nonprofit organization, oversees the creation, promulgation, and use of thousands of norms and guidelines that directly impact businesses. ANSI's work involves IT and health care, demonstrated by its approval of a standard around access control[67] and its involvement and sponsorship of HITSP.[68] The Identity Theft Prevention and Identity Management Standards Panel (IDSP) task force focuses on facilitating the use of voluntary consensus standards and guidelines to minimize the scope and scale of identity theft and fraud.[69] The IDSP released a report in January 2008 that identified standards, guidelines, and best practices related to identity theft and fraud prevention, with some information related to the exchange of health information and medical identity theft.[70] Among many other recommendations, the report suggested improvements to patient identity verification processes, security standards for handling electronic health records, and maintaining the privacy of patient information, all of which are intended to reduce the occurrences of privacy and security incidents, including medical identity theft.

On May 10, 2006, Executive Order 13402 established the *President's Task Force on Identity Theft* was established by Executive Order 13402 on May 10, 2006. The task force was composed of the Secretaries and Directors of 17 federal agencies, including DOJ, FTC, the Department of Treasury, HHS, the VA, the Department of Homeland Security, and others. It was charged with, among other duties, assisting the federal government in deterring, preventing, detecting,

---

65 Healthcare Information Technology Standards Panel, TN900 - HITSP Security and Privacy Technical Note. http://www.hitsp.org.

66 Certification Commission for Health Information Technology. http://www.cchit.org.

67 ANSI INCITS 359-2004, American National Standard for Information Technology; Role Based Access Control http://csrc.nist.gov/groups/SNS/rbac/

68 ANSI Standards Activities: Healthcare Information Technology Standards Panel. See http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3

69 The American National Standards Institute. Standards Panels and Forums: Identity Theft Prevention and Identity Management Standards Panel

70 ANSI-BBB Identity Theft Prevention and Identity Management Standards Panel. Final Report: Volume 1 Findings and Recommendations. January 31, 2008.

investigating, and prosecuting identity theft through law enforcement, education, and security safeguards provisions. The *President's Task Force on Identity Theft* issued its Strategic Plan on April 11, 2007. Among its many recommendations, the Strategic Plan provided guidelines for making consumer data more challenging for thieves to access, developing victim recovery programs, and deterring future occurrences of identity theft by developing more aggressive prosecution and punishments for those who commit the crime. In addition, the Strategic Plan acknowledged that identity theft cannot be eliminated by any one solution because it requires a comprehensive strategy. This strategy includes prevention, awareness, victim assistance, greater involvement by law enforcement, and coordination among federal, local, and state governments as well as the private sector. Although the task force did not extensively consider medical identity theft, there was information recognizing the issue, and many of the overall findings of the task force are relevant to understanding and addressing medical identity theft.[71]

In addition to the work of these entities and others, industry responses to the need for health IT privacy and security have been significant. In recent months, for example, private companies have acknowledged the public's interest in health IT privacy and security by emphasizing these features in products offered directly to individual consumers. Some large, well-known companies with broad resources and public name recognition now offer tools such as PHRs to consumers. The services and functionality of these tools vary, but all seek to empower consumers with the ownership and management of their own health information. Several of these commercial vendors recognize their potential customers' interests in maintaining privacy and security issues. This recognition is evident from the placement and messaging on their websites concerning vendor privacy, security, and data sharing policies. Such policies that affect medical identity theft include the privacy and security functionalities of the tools and products themselves.

6.0 MEDICAL IDENTITY THEFT: CURRENT POLICIES AND PROCEDURES

Further developments in health IT and privacy and security-related efforts may leverage best practices from other industries. Many of the documents that were reviewed and stakeholder perspectives collected for the environmental scan referred to the financial industry in particular as a potentially valuable point of comparison to the health care industry. The major lesson available from the financial industry, however, appears to be that no single solution will adequately prevent identity theft. Stakeholders in the financial industry have dedicated significant time and resources in determining where and how privacy and security breaches occur and in identifying patterns and trends. The results of this research included developing unique credit card security identifiers, requiring picture identifications when conducting transactions, implementing audit logs that track access, identifying transaction anomalies, and developing education and awareness tools and materials. While many of these solutions appear to be feasible in the health care industry, it is in the nascent stages of developing comparable responses. We discuss the comparable approaches below. Appendix B contains detailed information about existing laws that relate to the rights and obligations of medical identity theft stakeholders.

[71] Presidential Identity Theft Task Force: Strategic Plan. Medical Identity Theft, pg 20. http://www.idtheft.gov/reports/StrategicPlan.pdf.

6.1 MEDICAL IDENTITY THEFT PREVENTION

Prevention methods specific to addressing the issue of medical identity theft are in the early stages of development, and in most cases, organizations have yet to consider the unique aspects of medical identity theft as a part of their overall risk assessment. Many of the preventive measures that either are business standards from other industries or have more recently been developed in the context of health IT are being deployed in health service entities and may provide guidance to mitigate the threat of medical identity theft.

Preventing medical identity theft is preferable to responding to it for several reasons. Prevention minimizes risk to patients' health records by decreasing the possibility of inappropriate information being inserted into an individual's record. Many stakeholders interviewed believe that prevention can be less expensive than remediation because some relatively low-cost preventive techniques can avoid incidents that are far more costly to a program or system.[72] We discuss some examples of these existing solutions below. Some have not been implemented very broadly but may warrant further study.

6.1.1 Risk Assessment[73]

As an early step in developing a robust information security program, many organizations (including all federal agencies) conduct a risk assessment. The National Institute of Standards and Technology (NIST) defines a risk assessment as "the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system."[74] The definition further explains that a risk assessment is "part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls."[75] The risk assessment process can help to define preventive measures to reduce the likelihood of medical identity theft occurring in addition to developing appropriate responses if it does occur. HIPAA Security Rule also requires covered entities[76] to "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (PHI).[77]

---

72 One case study, for example, determined that a fraud detection strategy yielded a 755 percent return on investment and a 370 percent savings improvement in its first year of implementation. See Ingenix, Inc., "United Healthcare Prevents Fraudulent Claims Payments and Saves Nearly $125 Million with Ingenix Prospective Fraud Detection Solutions," 2007 (available at http://www.ingenix.com/content/attachments/06-10298%20UHC%20Case%20Study.pdf). Similarly, one interviewee noted that a fraud detection program instituted resulted in a 15-to-1 return on investment. Neither of these programs was limited to medical identity theft alone.

73 Several sources use the terms "risk assessment" and "risk analysis" interchangeably, and ONC will in this document as well.

74 NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, July 2002, provides guidance, mandatory for federal agencies, on how to conduct a risk assessment.

75 Ibid.

76 Covered entities are the individuals and organizations on whom the HIPAA Privacy and Security rules place certain direct obligations. They are defined in the rules as including "(1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." See 45 CFR § 160.103. The rules also place enforcement and oversight obligations on various federal agencies and require covered entities to place further obligations on their "business associates," some of whom may also be vulnerable to medical identity theft.

77 68 Fed.Reg. 8333, "Health Insurance Reform: Security Standards; Final Rule" (hereafter "HIPAA Security Rule), p. 8377; codified at 45 CFR § 164.308(a)(1)(ii)(A).

Risks, threats, and vulnerabilities[78] are not inherent in the technology and physical infrastructure alone. Health care fraud in general and medical identity theft in particular occur because of the behaviors of people. Gaps in an organization's policies also may contribute to a situation that allows medical identity theft to occur. Organizations with comprehensive and effective risk assessment programs consider all of these issues—people, technology, and policy.[79]

6.1.2 Training, Education, and Awareness

Some affected institutions have begun to provide training, education, and awareness to staff members related to medical identity theft. According to a number of interviewees and much of the literature, however, neither consumers nor health care providers have an adequate level of awareness and understanding of medical identity theft and the risks associated with it, nor do they have a full understanding of the costs incurred once medical identity theft has occurred. While HIPAA-covered entities are required to "implement a security awareness and training program for all members of its workforce (including management),"[80] many interviewees concurred that medical identity theft is not often addressed in these programs as a separate and unique topic or risk.

In addition to using education and training as a preventive measure, many covered entities conduct training after an incident to verify that workforce members and contractors have responded appropriately. Conducting education and awareness activities following a medical identity theft incident allows staff to debrief, identify and apply lessons learned, and continually improve the quality of privacy and security process and procedures.

Some institutions that have conducted education and awareness programs on medical identity theft included consumers and health care organization employees in their efforts. These groups note that including consumers may be an effective detection method because in many cases, consumers learn that their information has been misused before their health care providers, insurance plans, or any other stakeholders. Because consumers and caregivers are in the best position to know what services they received, they will be able to identify fraudulent or incorrect health information within their medical records. As a result, some insurance providers are now encouraging enrollees to practice the same preventive measures against medical identity theft that they use against financial identity theft. These measures include reviewing records of recent interactions with the industry and providing the same protection for their medical plan enrollment cards that they do for their credit cards.[81]

6.1.3 Patient Authentication

Many health care providers now ask patients to provide a separate form of identification in addition to health insurance coverage information to verify their identity. Some require this

---

78 See NIST 800-53, *Recommended Security Controls for Federal Information Systems* (December 2006), for definitions of "threat," "vulnerability," and "risk."

79 AHIMA e-HIM Workgroup on Medical Identity Theft. "Mitigating Medical Identity Theft." *Journal of AHIMA* 79:7 (July 2008): 63–69.

80 HIPAA Security Rule, p. 8377; codified at 45 CFR § 164.308(a)(5)(i).

81 Studies have shown that consumers are familiar with the implications of financial identity theft, but few are aware of the facts surrounding medical identity theft. For example, EpicTide, a provider of security systems for the health care industry, conducted a survey that concluded consumers are unfamiliar with the potential consequences associated with medical identity theft and have a narrow understanding of health privacy laws. See Crane, Amy Buttell. "Medical Identity Theft Can Kill You." Bankrate.com, February 11, 2007.

additional authentication at the first patient visit, whereas others require it at every visit. Many stakeholders interviewed cited this practice, known as patient authentication, as a key method of combating medical identity theft. Some noted that requesting identification alone may serve as a deterrent to attempting medical identity theft in cases where a perpetrator will not be able to produce appropriate identification, as in cases where the perpetrator has the consumer's information but not their identity cards or other documentation.[82]

Health care providers have used other technology solutions that may have had the effect of reducing medical identity theft, although the intent of implementing such solutions may not have been specifically focused on medical identity theft. For example, a "smart card" system was adapted by a health care network in Queens, New York. According to a newsletter from the Smart Card Alliance "smart cards help reduce health care paperwork and secure access to patient records and health insurance status. The smart card is an ideal medium for holding encrypted patient information, and for computing a digital signature or a biometric template to reduce ambiguity about the cardholder's identity." Each patient in this network carries a card that contains data such as the patient's name, address, emergency contacts, allergies, current medications, and recent lab results. To verify their identity, patients' cards are scanned similar to the way credit cards are scanned. Therefore, a medical identity thief cannot assume the patient's identity unless the thief has the individual's smart card. These protections will prevent potential medical identity thieves from using another's identity in cases of nonconsensual medical identity theft.[83] To date, these hospitals have issued cards to thousands of consumers. Similarly, a university medical center has implemented smart card technology and has distributed this "Health care Passport" to more than 2,000 patients. To access health information, the provider or patient must have the Health care Passport and a personal identification number (PIN) to access the information encoded on it. This safeguards protects against unauthorized access in the case a smart card is lost.[84]

[82] The HIPAA Privacy Rule does not require patients to provide authentication for the purposes of receiving health care services. It does, however, require covered entities to verify the identity and authority of individuals requesting access to protected health information, which may assist health care organizations in preventing medical identity theft. See 45 CFR § 164.514(h)(1).

[83] Identity thieves, however, do succeed in obtaining personal identification numbers (PIN) through methods such as social engineering. For this method to be effective, PINs must be kept secret, and neither disclosed to others nor written down anywhere they can be inappropriately accessed.

[84] Smartcard Alliance, "Smart Card Applications in the U.S. Health Care Industry," Smartcard Alliance Newsletter February 2006. Available at http://www.smartcardalliance.org/newsletter/february_2006/feature_0206.html.

Some interviewees noted, however, that patient authentication methods also pose risks. In one case, the thief had stolen the individual's driver's license as well as her insurance information. Once the victim discovered the theft, she had difficulty in proving that she had not received the services because the health care facility had a scan of her driver's license on file and believed that the victim had provided it at the time of care. At that time, medical staff could have discovered the medical identity theft if they had taken a closer look at the license photo. This incident illustrates that patient authentication must be implemented effectively, so it does not contribute to the complexities of the problem. More specifically, it illustrates the frequently observed principle that policies, procedures, and technology are only effective in combating medical identity theft if providers and staff receive and adhere to appropriate training and awareness.

Many health care facilities that request patient identification have noted positive results: A university health center in Connecticut developed a patient authentication policy after an incident of medical identity theft resulted in the loss of over $76,000 in services. Hospital administrators required anyone seeking treatment to produce photo identification. An official at the university notes "We've since had instances where patients say, 'I left my ID in the car,' then leave and never return." She says the center will begin scanning photo identification into their files to assist staff in verifying the patient's identity on subsequent visits.[85]

To date, these methods have mostly been effective when an individual attempts to commit medical identity theft and the demographics do not match those of an existing record. Some interviewees recalled incidents of refusing to accept insurance information when the thief was clearly of a different race, gender, or age than the individual whose health record the thief attempted to use while trying to get care.[86]

6.2 MEDICAL IDENTITY THEFT DETECTION

From our literature search and the interviews conducted, it is clear that medical identity theft is difficult to detect. Once the theft occurs, detecting services delivered to an impostor from services delivered to an individual whose identity has been stolen may be hard to distinguish. As a result, the amount of time that elapses between when an incident has occurred and when it is discovered may be significant.

Some methods of detection require resources and systems that can be expensive to obtain and implement; consequently, they are not appropriate for all types of providers. Detection may be slightly easier, however, in cases where changes are obvious in billing patterns. For example, when a sizable number of records are stolen for the purposes of submitting a large batch of false claims, sudden "spikes" in activity may elicit suspicion. Isolated incidents may be difficult or impossible to detect unless victims review their records and notice discrepancies.

Based on our research, most health care delivery organizations maintain some form of privacy and security program, either pursuant to HIPAA standards and/or as a matter of best practices, but may not have considered medical identity theft. Many interviewees noted that the victims themselves are usually the first to discover when medical identity theft has occurred and report it to their providers or insurers.

[85] ABC News, "Medical ID Theft Can Wreck Victims' Health and Finances" (May 3, 2006), retrieved September 7, 2008.

[86] Note that in these circumstances, the care provider may still be required to treat the individual under federal or state law. Refusing to treat someone under another's identity is distinct from refusing to treat that individual. We are not aware of any trend toward refusing care as a result of discovering attempts at medical identity theft.

6.2.1 Bill Notices or Collection Agencies

The financial industry has tools in place for consumers to check their financial standing through their credit report. The Fair Credit Reporting Act (FCRA) allows individuals one free report per year from each of the three nationwide consumer reporting agencies.[87] As another option, they can sign up through a number of agencies to receive more frequent monitoring ability, plus alerts, for a monthly fee.

When individuals become victims of financial identity theft, they may be able to detect the fraud through their credit reports showing instances of new bank accounts or outstanding payments. In the alternative, individuals may discover suspicious activities by monitoring their own individual accounts. In fact, according to an FTC 2006 survey, 37 percent of all identity theft victims "discovered the misuse of their personal information by monitoring the activity of their accounts."[88]

Victims of medical identity theft, however, do not have separate tools—e.g., ones that track all interactions with the health care system in a centralized record that can be monitored for irregularities—available to them.[89] Instead, often victims will receive a bill for health care services not rendered or a notice from a collection agency before they become aware that their identity has been stolen.[90] In cases where consumers suspect they have become victims of medical identity theft, they can use their rights under the HIPAA Privacy Rule to access their health records and request amendments for any inaccuracies.[91]

6.2.2 Explanation of Benefits

Insurers often provide explanation of benefits (EOB) to consumers to summarize medical services received[92] and tie the appropriate identification codes to health insurance claims. The contents of this document reflect the data that insurers use to determine whether the claim is covered by the consumer's insurance policy or program and whether the consumer is responsible for any co-payments or other costs.

Many of the people interviewed in the course of this environmental scan expressed the opinion that EOBs could be a valuable tool in detecting medical identity theft.[93] Patients can review EOBs and determine that their providers and payers have accurate records of their interactions with the health care system. This review is an opportunity for the patient to verify that the description of services provided and other information on the EOB are accurate.

---

87 A recent amendment to the federal Fair Credit Reporting Act requires each of the nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to provide you with a free copy of your credit report, at your request, once every 12 months. http://www.ftc.gov

88 *Federal Trade Commission – 2006 Identity Theft Report*. Prepared by Synovate, November 2007. http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

89 Health care consumers, however, can use the Privacy Rule's rights of access and accounting similarly to their use of credit reports to ensure the accuracy of their medical information. See 45 CFR §§ 164.524 and 164.528.

90 Dixon, Pam. "Medical Identity Theft: The Information Crime that Can Kill You." World Privacy Forum. May 3, 2006.

91 See HIPAA Privacy Rule, 42 CFR § 164.524 (Access of individuals to protected health information) and 42 CFR § 164.526. (Amendment of protected health information), discussed in footnote 40.

92 Some insurers provide EOBs only if the patient is financially responsible for any portion of the costs of care they receive.

93 See for example Blue Cross/Blue Shield's "Interactive Explanation of Benefits," which educates consumers on how to read their EOBs and determine whether they have been the victims of medical identity theft. See http://www.bcbs.com/blueresources/anti-fraud/explanation-of-benefits.html, retrieved September 7, 2008.

There are barriers, however, to the effectiveness of this approach in detecting medical identity theft. EOBs often contain medical and insurance community terminology, and terms can be uncommon and unfamiliar to most consumers. Therefore, consumers may not be able to correlate what they see on the EOB with the medical services they received. Also, in many cases, EOBs are issued to consumers up to 90 days after services are received. Consumers are less likely to remember what services they have received if several months elapse before they review the EOB, thus reducing their ability to detect anomalies. Many interviewees noted that the EOBs are often difficult to read and understand and consumers often do not read them. However, on occasion, consumers were able to detect inaccuracies through these reports.[94]

6.2.3 "Red Flag" Approaches

Much like the financial services industry, the health care industry handles large volumes of transactional data, and stakeholders have examined the financial sector for privacy and security best practices. Under a "red flag" approach, for example, an organization establishes a protocol for identifying a suspicious pattern of activity and conducting appropriate follow-up.

This approach is currently used in the financial industry. The current Red Flags Rule is a joint regulation published in November 2007 by several federal agencies.[95] The rule was required under the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which itself amended the FCRA. The rule requires "financial institutions" and "creditors" with certain types of "covered accounts" to develop and implement a written plan to identify "Red Flags," or patterns, practices, or specific activities that indicate the possible existence of identity theft. This rule does not stipulate the specific requirements of such a plan but rather requires subject entities to develop plans appropriate to their size, complexity, and the nature and scope of their activities. Thus, the rule is intended to be flexible to meet the needs and nature of the applicable health care entities. Examples of possible Red Flags include warnings or notices provided to the entity from a consumer reporting agency or credit bureau, warnings or notices provided to the entity from consumers who are victims of identity theft, suspicious changes of address, or unusual uses or activities in covered accounts. The Red Flags Rule is currently effective, with compliance required by November 1, 2008.

It is important to note that this rule defines key terms such as "financial institutions," "creditors," and "covered accounts" broadly and therefore would include entities outside of traditional financial institutions, including entities involved in the health care industry. In fact, many institutions in the health care industry may fall within the definition of "creditors" with "covered accounts"; therefore, they may be required to develop a written Red Flags plan. Though there are many ways to comply, it is expected that many health care entities will identify red flags of identity theft through new or existing internal controls.

---

94 World Privacy Forum cited "a mother checked her mentally ill son's explanation of benefits to find that Medicare had been billed for more than 70 respiratory treatments, even though her son did not have a respiratory condition." (p. 35)

95 The involved agencies include the Office of the Controller of Currency, the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission.

6.2.4 Data Analytics

Conceptually related to a Red Flags approach is the use of "data analytics," or "quantitative fraud prediction models."[96] These terms refer to an organization using data from past transactions to observe patterns and trends. In the health care context, "transactions" can include receipts of services, submissions of claims for reimbursement, or payments. Payers can then analyze or examine these transactions and the related data to detect when patterns of usage or payments may seem suspicious. For example, payers may analyze transactions and note a suspicious pattern if services requested or received are—

- Inappropriate for the patients' demographic (e.g., women's services for men, pediatric services for adults)
- Treatments for conditions with which patients have not been diagnosed
- Prescriptions for drugs that do not appear to be necessary and appropriate for the patient
- Receipt of prescriptions in unusually high frequencies, seen when patients are attempting to procure pharmaceuticals for abuse or resale.

Another method of data analytics involves identifying two or more records, supposedly for the same individual, with inconsistent demographic information. For example, records from two separate occasions of treatment for the same individual showing different dates of birth could indicate that the treatment was actually received by two separate individuals. Similarly, patterns of requests to change other demographic information may signal an opportunity to conduct further identification and verification. In the financial services industry, identity thieves often try to report a change of address to receive checks and other benefits. In this way, data analytics and Red Flags Rule compliance may blend, and models to detect anomalies in transaction data could become Red Flag tools for identifying possible occasions of medical identity theft.

In another overlap with fraud detection tools from the financial services industry, some interviewees referred to the process of developing an electronic algorithm to detect apparently erroneous or suspicious data patterns. Users may set up an automated process to take certain actions when these patterns occur. This process is often called "placing edits on the system." Users may place an edit on the system to detect an attempt to use an identity that is already known to be stolen. After the initial incident, further use of the victim's credentials trigger a notification to the insurer and provider. Such edits on the system have been used to detect medical identity theft, particularly in cases where thieves used multiple attempts to obtain drugs. In such cases, the edits on the system have notified pharmacies and providers in advance and have enabled them to assist in apprehending medical identity thieves. This process of placing edits on the system is similar to the process for placing fraud alerts on credit reports, as provided by FCRA.[97] Placing edits on the system can serve a similar purpose when using the information that a health care payer or provider collects on a patient to ensure that person's information is not misused or exploited by another.

Among its disadvantages, however, data analytics raises some concerns among consumers, privacy advocates, and others. Analyzing the information of a large group of people to detect

[96] Other terms for similar activities include "behavioral profiling" and "data mining."

[97] See 15 U.S.C. § 1681c-1(a)(1). With fraud alerts, individuals who suspect they are or are about to become a victim of financial identity theft can place an alert on their credit report. This alert requires creditors using that credit report to confirm or verify the identity of an individual before making certain changes to the credit status, such as extending a new line of credit or raising the limit on an existing line of credit.

possible criminal activity by a few can create an atmosphere of suspicion and discomfort, especially in cases where that analysis can result in "false positives," These particular cases may indicate criminal activity where none has occurred. Also, as a general privacy principle, health information disclosure is best limited to those purposes for which the data was collected. The HIPAA Privacy Rule, for example, reflects this principle by stating that a covered entity "may not use or disclose protected health information, except as permitted or required" by the HIPAA Privacy Rule, and describes in detail what categories of use are and are not permitted and required.[98] Some disagreement exists about whether using data analytics for the purposes of detecting criminal activity constitutes minimum use or not.

6.2.5 Civil and Criminal Investigations

A number of law enforcement agencies investigate and/or prosecute medical identity theft. These agencies include the HHS-Office of the Inspector General (OIG), Federal Bureau of Investigation (FBI), State Medicaid fraud control units, U.S. Attorneys Office, State Attorney Generals, FTC, the HHS OCR,[99] CMS, among others. In gathering evidence, agency investigators use a number of techniques, including conducting interviews and site visits, reviewing records, and conducting computer forensic investigations to determine who accessed electronic records, at what time, and what information was accessed. In some instances, victims may be notified of potential medical identity theft based on a criminal investigation. During the 1990s, a woman discovered that her psychiatrist had been billing her insurance company for providing services to her children. No such services were delivered. She later learned that the billing was not merely accidental because federal authorities were already investigating the psychiatrist for 136 counts of fraud.[100]

6.3 MEDICAL IDENTITY THEFT REMEDIATION[101]

For the purposes of this environmental scan, "remediation" refers to the process of responding to medical identity theft to reduce or eliminate its harmful effects. Based on interview feedback, remediation guidelines, processes, and procedures specific to medical identity theft have yet to be fully developed or broadly implemented. While organizations like AHIMA[102] and the World Privacy Forum[103] are exploring medical identity-specific remediation approaches, responses are not yet as mature as those of the financial industry or of the health care industry to other forms of health care fraud.[104]

---

98 HIPAA Privacy Rule, 45 CFR § 164.502, Uses and disclosures of protected health information: general rules.

99 The DOJ may also be involved. When OCR receives a complaint under the Privacy Rule, with facts alleging medical identity theft, it makes a referral to DOJ for criminal investigation. OCR also may initiate a civil investigation to determine whether covered entities have implemented adequate and reasonable safeguards to prevent medical identity theft.

100 "Diagnosis: Identity Theft." *Business Week*. January 9, 2007. http://www.businessweek.com/magazine/content/07_02/b4016041.htm

101 In this document, we use the term "remediation" to refer to efforts to respond to a medical identity theft incident and return the health care provider, plan, patient, and all other stakeholders to the same state they were in, as appropriate, before the event occurred.

102 American Health Information Management Association http://www.ahima.org.

103 World Privacy Forum http://www.worldprivacyforum.org.

104 The Privacy Rule's administrative requirements, however, address mitigation and sanctions, which may assist in the remediation of medical identity theft. See 45 C.F.R. § 164.530(e)(1) and (f). A covered entity's notification of the patient and other potentially affected entities, for example, would be considered part of a covered entity's mitigation activities.

6.3.1 Application of Sanctions

In anticipation of a potential security incident, including those that result in medical identity theft, organizations must develop policies and procedures concerning sanctions for inappropriate activity, ranging from warnings, to revoking individuals' ability to access information systems if they have misused that access, to termination in cases of willful and illegal activity. HIPAA-covered entities, for example, are required to "[a]pply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity."[105] In cases where a health care provider has participated in fraudulent activity, health care agencies and insurance companies often withdraw other privileges, such as not allowing the provider to use his or her provider billing numbers or revoking participation in the insurance network.

6.3.2 Post-Incident Auditing

In the event of a security incident, including those that result in medical identity theft, most affected entities make an attempt to identify how the inappropriate access and disclosure of patient data occurred. These activities may assist the entity in recouping losses, determine how to prevent breaches in the future, and contribute to an overall deterrent effect. If records are kept electronically, internal or external subject matter experts sometimes can determine whether audit logs have been erased or compromised and ensure that this information is available for the evidentiary record. HIPAA-covered entities are required to "implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information"[106] and to regularly review that record (specifically, to "regularly review records of information system activity, such as audit log […]").[107] In addition, business associates[108] of HIPAA-covered entities must "[r]eport to the covered entity any security incident of which [they] become aware,"[109] including those resulting in medical identity theft. If these security incidents constitute a "material breach or violation of the business associate's obligation under the contract or other arrangement, the covered entity must take reasonable steps to cure the breach or end the violation."[110] These requirements may create an obligation on the part of the covered entity to identify the cause of an incident resulting in medical identity theft that occurred because of the actions or inactions of a business associate and ensure that any security vulnerability has been adequately addressed.

---

105 HIPAA Security Rule, Sec. 164.308(a)(1)(ii)(C).

106 HIPAA Security Rule, Sec. 164.312(b).

107 HIPAA Security Rule, Sec. 164.308(a)((1)(D).

108 A "business associate" under the HIPAA Privacy and Security Rules is "a person who, …, on behalf of such covered entity or of an organized health care arrangement (as defined [under the Privacy Rule]) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of…A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or…[a]ny other function or activity regulated by this [45 CFR Subtitle A, Subchapter C], or…[p]rovides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501 of [45 CFR Subtitle A, Subchapter C]), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person….A covered entity may be a business associate of another covered entity." See HIPAA Privacy Rule, 45 CFR § 160.103.

109 45 CFR 164.314(a)(2)(i)(C).

110 45 CFR 164.314(a)(1)(ii).

6.3.3 Law Enforcement

One response to medical identity theft is to involve law enforcement officials in identifying thieves, and ideally, their prosecution. The HHS OIG, FBI and state Medicaid fraud control units are the primary law enforcements agency for investigating allegations in health care fraud. The Criminal Division of the U.S. DOJ prosecutes more than 700 cases of health care fraud every year. Although the number of these cases that involve medical identity theft are not known, law enforcement officials may be able to recoup large losses, prevent further activities by organized rings, and provide deterrence for future offenders.

To ensure that DOJ and other enforcement officials are advised of incidents that may be appropriate for investigation and prosecution, health care organizations often refer incidents of medical identity theft to one of several authorities. Many state attorneys generally maintain health care fraud offices, and cases of medical identity theft can be referred to them for investigation. The National Association of Attorneys General maintains a referral service at www.naag.org. The FTC also operates an Identity Theft Clearinghouse, available at www.ftc.gov, which collects consumer identity theft complaints that can be accessed by law enforcement. The HHS OIG maintains a hotline for reporting fraud, including Medicaid and Medicare fraud, (800-HHS-TIPS) and maintains a website with many other resources at http://www.oig.hhs.gov/hotline.html. Finally, HHS OCR[111] may be able to assist in its role as the enforcement agency for the HIPAA Privacy Rule, or CMS may be able to assist in its capacity as the agency with responsibility for enforcing the HIPAA Security Rule. This assistance includes investigating allegations that medical identity theft has been a result of inappropriate privacy and/or security controls that do not satisfy the requirements of the HIPAA rules. Furthermore, OCR and CMS may refer complaints that allege potentially criminal violations to the attention of the DOJ.[112]

Local law enforcement agencies, such as police departments, sometimes may become involved in medical identity theft cases. This case is especially true where the dollar value of the medical identity theft incident is low, and the incident does not involve interstate transactions or businesses, and federal agencies do not have jurisdiction. Local agencies, however, may not be familiar with medical identity theft or may not have the resources to investigate it thoroughly. For example, in cases involving hacking and other cyber crimes, investigation may require expertise and interagency collaboration that are beyond the scope of a local agency's capabilities.[113]

6.3.4 Advise Potentially Affected Entities

Another activity to conduct in the wake of a breach involves ensuring that any inaccurate information introduced into the victim's medical record has not been forwarded to other data users. To determine the date that incorrect information entered the record—and to identify to whom the corrupted record was disclosed—providers or affected individuals often contact the "downstream" record holders and advise them that the records may contain inaccuracies. In fact, under the HIPAA Privacy Rule, covered entities "must make reasonable efforts to inform and

---

111 The OCR may be contacted via its website at www.hhs.gov/ocr.

112 ONC thanks Harry Rhodes of AHIMA for assembling this contact information.

113 Jim McKay, "Identity Theft Steals Millions from Government Health Programs," Government Technology, February 13, 2008. Available at http://www.govtech.com/gt/260202.

provide the amendment within a reasonable time to…[p]ersons identified by the individual as having received protected health information about the individual and needing the amendment; and … [p]ersons, including business associates, that the covered entity knows have the protected health information that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual."[114] Several interviewees noted that this process can be time-consuming and difficult because providers may be reluctant to alter records. Providers may choose merely to annotate the record to indicate the disputed information, which may allow errors to remain in health records despite efforts to remove them.[115] In fact, in a few states, changes or corrections to health records must be made in accordance with state laws that forbid deleting the information. As noted in a recent AHIMA publication: "In Arkansas, errors on hard copy medical records must be corrected by drawing a single line through the incorrect entry, labeling the entry as an error, and initialing and dating it.[116] In Massachusetts, health care facilities may not erase mistakes, use ink eradicators, or remove pages from the record."[117] [118]

6.3.5 Patient Notification and Access

Notification to potentially affected individuals is one of the most common responses to information security incidents. At least 44 states, the District of Columbia, and Puerto Rico require companies doing business in that state to advise residents when their information may have been compromised, and many of these impose further responsibilities on those businesses as well.[120] California was the first state to require such notification,[121] and it recently amended that law to explicitly address health care organizations.[122] As set out, this California law requires that "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal

Consumers may not even know their records have been compromised:
In January 2008, the state of California enacted a law that requires providers to notify consumers when their medical information has been "breached." But only a handful of other states spell out notification requirements regarding unauthorized release of patient medical data. In contrast, most states have so-called breach notification laws that address accidental disclosures of financial information; these also may apply to medical data in certain instances.[119]

[114] HIPAA Privacy Rule, 45 CFR 164.526(c)(3).

[115] While individuals have the right under HIPAA to have a covered entity amend protected health information or a record about the individual in a designated record set, covered entities may deny an individual's request for amendment if they "determine that the protected health information or record that is the subject of the request…[w]as not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment; …[i]s not part of the designated record set; … [w]ould not be available for inspection under [45 CFR] § 164.524; or [i]s accurate and complete. See HIPAA Privacy Rule, 45 CFR 164.526(a)(2).

[116] Ark. Code 14(A)(6). See also N.J.Admin.Code tit. 8, s. 8:43G-15.2(l) ("corrections shall be made by drawing a single line through the error and dating the correction").

[117] 105 Code Mass. Regs. 150.013(B).

[118] Roach, William H.. Medical Records and the Law. Fourth Edition. Sudbury, MA: Jones and Bartlett Publishers, Inc., 2006.

[119] Andrews, Michelle. "Medical Identity Theft Turns Patients Into Victims." *US News World and Report*, February 29, 2008.

[120] See, e.g., the National Conference of State Legislatures, "State Security Breach Notification Laws," http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (updated June 20, 2008), last retrieved September 7, 2008.

[121] California Senate Bill (SB) 1386

[122] See California AB 1298, (February 3, 2007), which requires "[a]ny agency that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The bill defines "personal information" to include "medical information" as well as "health information." Ibid.

information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." In addition, this law permits delayed notification "if a law enforcement agency determines that [immediate notification] would impede a criminal investigation."[123]

Many of these state laws further require companies to offer individuals credit monitoring services in the event of a breach. Because these laws are still relatively new, evidence is lacking on their effectiveness in preventing identity theft. One report released this year suggested that they have no statistically significant impact in reducing identity theft.[124] This type of legislation, however, provides an incentive for companies to improve security controls and allows consumers to make informed decisions about their individually identifiable information.

In the case of medical identity theft, it may also be possible to provide greater access to patient records to allow individuals to determine whether their health care data has been used inappropriately to access services. Patients have the right to request copies of their medical records under the HIPAA Privacy Rule.[125] Also, some organizations provide copies of affected patients' medical records following a breach so individuals can detect any inaccuracies. This provision is accomplished by—

- **Providing EOBs.** Health care plans often provide recipients with statements reflecting what services have been received and by whom. Some insurance plans also provide, on each EOB, information on the actions the recipient can take if the information is inaccurate.
- **Providing full copies of the medical record.** Hard or electronic copies of records are often made available to individuals for their review.

In addition to these notification procedures, providers or plans whose records have been breached sometimes validate the information in the health records they maintain or use. This validation compares name, address, and other demographics with patients' identification documentation.

6.3.6 Redress

Having provided notification and access, organizations also may need to ensure that individuals are returned, to the greatest extent possible, to the same position they were in before the breach occurred. Patients are normally provided methods of "redress," which is the ability to request and receive opportunities to correct changes in records or otherwise compensate them for the negative effects of the theft.[126] One method of redress often implemented is in providing frequent disclosures of patient records and account activity to ensure that compromised data is not used inappropriately. In addition, health care providers and plans often may provide patients with—

123 Ibid.
124 Romanosky, Sasha et al. *Do Data Breach Disclosure Laws Reduce Identity Theft?* Center for Digital Strategies, Tuck School of Business, Dartmouth College. June 2008.
125 HIPAA Privacy Rule, § 164.524 (Access of individuals to protected health information).
126 The term "redress" is often used in this sense when discussing privacy issues. In some legal proceedings, "redress" may refer to compensation received by victims. We will use it in the sense of allowing individuals to correct their records or otherwise receive compensation specifically for losses related to identity theft.

- **Mechanisms to seek corrections to their health records.** Individuals may wish to make requests to amend health information that has been improperly inserted into their records as a result of medical identity theft. Patients have the right to make this request under the HIPAA Privacy Rule.[127] For purposes of controlling their own liability and ensuring treatment delivered is appropriate, providers are allowed under the HIPAA Privacy Rule to refuse requests to amend patients' health records, although some may instead note in these health records that such requests were made.[128]
- **Mechanisms to receive an accounting of disclosures.** Under the HIPAA Privacy Rule, an individual "has a right to receive an accounting of disclosures of protected health information made by a covered entity in the six years prior to the date on which the accounting is requested," subject to some conditions and exceptions.[129] For each disclosure, the covered entity must note the date of the disclosure, the name and address (if known) of the entity or person who received the PHI, a brief description of the PHI that was disclosed, and a brief statement of the purpose of the disclosure.[130]
- **Advice on how to contact appropriate offices and what these agencies can do.** Patients can contact offices such as the FTC, HHS OIG, CMS, HHS OCR, and SSA.
- **Credit monitoring.** While financial identity theft is beyond the scope of this document, credit monitoring could conceivably serve as a method of detecting subsequent, further medical identity theft. If individuals are unaware services are being delivered to someone under their identity, they may default on charges for medical goods or services. If creditors report delinquencies to a credit bureau, these individuals' experience with medical identity theft can, ultimately, affect their credit rating. Because some time may pass before medical identity theft affects credit rating, however, this method for detection may not be effective.

Correcting medical records in the wake of medical identity theft can be a time-consuming process. In the financial identity theft world, estimates of the time individuals require to address the issue are between 5 and 20 hours, although some individuals experience greater, unusual burdens. On the provider side, some commercial services can review records and verify they are accurate, but these services can take 5 to 20 hours per record to remediate, at a cost of nearly $200 per record.[131]

6.3.7 Change of Account Numbers

Individuals subjected to medical identity theft are often provided with new insurance account numbers and new user names and passwords for online access. Notably, where the victim is a Medicare patient, the Medicare account number uses the digits of the individual's SSN.[132] Changes to SSNs are difficult and rare because the system was designed to assign a single

---

127 See HIPAA Privacy Rule § 164.526 (Amendment of protected health information). The covered entity may refuse to make an amendment if (i) the covered entity determines that the protected health information or record that is the subject of the request is accurate or complete; and (ii) the covered entity identifies, and appends or otherwise links, the following pieces of information to the patient's record: the individual's request; the covered entity's denial of the request; the individual's statement of disagreement; and the covered entity's rebuttal. See HIPAA Privacy Rule § 164.526(a)(2)(iv), (d)(4).

128 See discussion of HIPAA Privacy Rule, 45 CFR § 164.526(a)(2) at footnote 112.

129 45 CFR § 164.528(a)(1).

130 45 CFR § 164.528(b)(2).

131 Ponemon, "2006 Annual Report" and Roop, Elizabeth S., "Fighting Fraud & Identity Theft in Radiology." *Radiology Today*, 7:23 (November 20, 2006), p. 40.

132 Consumer Union. "Social Security Numbers on Medicare Cards puts Consumers at Risk for Identity Theft" October 2004.

number to each individual that will remain constant over that person's lifetime. Changing an SSN may complicate that individual's future ability to navigate systems dealing with employment, banking and finance, tax, and public benefits.[133] Therefore, even when medical identity theft involving a Medicare account is discovered, it will not often be possible to change the account number. Consequently, medical identity thieves could continue seeking care and/or submit claims under the same Medicare account number even after medical identity theft has been detected.[134]

7.0 CONCLUSION

We identified many possible approaches in responding to medical identity theft, but much work remains. To help ensure the effects of this issue are addressed, future activities may include assessing the true scope of the problem, identifying appropriate solutions, and testing these solutions in appropriate environments, such as pilot programs and research studies.

Ultimately, effective solutions may need to be integrated into more widespread efforts. For example, where policy and procedure changes are necessary, stakeholders may wish to consolidate materials into appropriate documentation and training. In cases where technical solutions prove effective, system architectures may need to be modified to accommodate these solutions and to address appropriate risk assessment vulnerabilities.

While not all interviewees agreed on the probable frequency of medical identity theft and the magnitude of its effects, all agreed that it has not yet been accurately determined or even reliably estimated. Not knowing medical identity theft's extent prevents stakeholders from selecting appropriate responses. While many interviewees believe medical identity theft is on the rise, we note that this may be a perception rather than an actual trend. It may be the case that the frequency of medical identity theft has remained constant, but stakeholders are recognizing the problem more often. Future efforts in collecting better data on medical identity theft will be important to understanding the full impact of this issue.

We identified a number of possible methods of addressing medical identity theft that are already in place in some organizations. Efforts have increased to develop networks of health care providers to exchange data about patients; however, standard practices must be developed to ensure interoperability and clear expectations among business partners.

Health IT can provide an important and effective tool for the prevention, detection, and remediation of medical identity theft. The broad electronic exchange of health information most likely will require the creation of sizeable networks, and the implementation of these which carry both opportunities and risks related to medical identity theft. For example, one advantage of these large-sized networks is that they may provide opportunities for detection through auditing and electronic identity authentication. On the other hand, they may pose threats related to medical identity theft. First, the networks are able to maintain the records of many individuals. As a result, an identity thief could gain inappropriate access to a substantial number of health

[133] According to SSA "a new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."

[134] Social Security Administration. Electronic Leaflets "Identity Theft and Your Social Security Number."

records, including individuals who are geographically diverse, which enables exploits that affect many individuals with large financial impacts. Second, when medical identity theft results in the corruption of data in the health record, an electronic network can disseminate that incorrect information quickly and broadly. Depending on how information is tracked and stored, inaccurate health information could wind up in records controlled by many different entities. Medical identity theft victims could then find it even more challenging to remove mistakes in their records because the information could be spread across countless systems.

Consideration of medical identity theft, then, is timely and appropriate. An opportunity exists now to pinpoint the true scope of the problem, identify appropriate steps to mitigate the danger it poses to patients, and integrate those solutions into ongoing efforts to develop standards for the privacy and security of a Nationwide Health Information Network.

APPENDICES

APPENDIX A

Table A1: Stakeholder Interviews

Interviewee	Date (all in 2008)
Office of the National Coordinator	June 3
Federal Trade Commission (FTC)	June 13
Centers for Medicare & Medicaid Services (CMS)	June 13
Center for Democracy and Technology (CDT)	June 13
American Health Information Management Association (AHIMA)	June 19
Department of Justice (DOJ)	June 20
HHS Office for Civil Rights (OCR)	June 20
Healthcare Information and Management Systems Society (HIMSS)	June 24
Consumer Union	June 25
HHS Office of the Inspector General (OIG)	June 27
[Redacted]	June 30
National Governors' Association	July 1
Coalition Against Insurance Fraud	July 7
Blue Cross/Blue Shield Association of America (BCBSA)	July 8
[Redacted]	July 10
Kroll Fraud Solutions	July 11
National Health Care Anti-Fraud Association (NHCAA)	July 14
[Redacted]	July 21
Digital Harbor	July 23
Identity Theft Resource Center	July 24
American National Standards Institute (ANSI)	July 25
Good Health Network	July 28
Indiana Health Information Exchange	July 28
MedStar Health	July 28
Massachusetts General Hospital	July 29
[Redacted]	August 1
Office of the United States Attorney, District of Maryland	August 5
World Privacy Forum	August 7
Social Security Administration (SSA)	August 11
North Carolina Healthcare Information and Communications Alliance, Inc. (NCHICA)	August 21
CareSpark	August 22
Laurinda Harman, Temple University	August 27
Summit Health Institute for Research and Education (SHIRE)	August 27
American Hospital Association	Sept 4
Michigan Health Information Alliance	Sept 4
Hospital Corporation of America	Sept 5

APPENDIX B

Existing laws that affect the rights and obligations of medical identity theft stakeholders.

Table B1: Existing Laws

Title	Citation	Affected Stakeholders	Key Provisions
Common law	Law created and implemented by the judicial branch reflecting legal traditions and prior case law	• Any person or organization with a duty to protect the personal information of another • Individuals whose information is collected, used, transmitted, stored or disclosed by a person or organization that may be sued under the laws of the United States	Suits for negligence may allow individuals to recover monetary damages under state law if those with a duty to protect their information (either under contract, law, or any other legal concept) provide inadequate protection or are otherwise responsible for an inappropriate disclosure that results in harm to the individual.
Federal Trade Commission Act of 1914	15 U.S.C. §§ 41-58, as amended	Persons, partnerships, and corporations (with some exceptions)	• Acts against unfair or deceptive trade practices. • In an information assurance context: – An unfair practice might include not providing reasonable security for customers' personal information, where such failure causes or is likely to cause significant consumer injury – A deceptive practice might include not providing privacy or security protections promised or advertised • Remedies include injunctive relief to prohibit or mandate particular practices • Generally does not provide for regular damages; provides for civil penalties only for violation of obligations specified by rule or certain statutes, or of prior order
Health Insurance Portability and Accountability Act (HIPAA) Security Rule	*Health Insurance Reform: Security Standards; Final Rule*. 68 Fed.Reg. 8333 (February 20, 2003). Codified at 45 CFR Parts 160, 162, and 164.	• HIPAA covered entities (organizations that conduct certain kinds of transactions electronically and are): – Health care plans – Health care providers, or – Clearinghouses, as these terms are defined by the Security Rule • Patients and consumers of health care	• Requires covered entities to implement Administrative, technical, and physical safeguards for the protected health information (PHI) under its control • Provides penalties for knowingly violating HIPAA: – Fines up to $50,000 and prison terms up to 1 year – Fines up to $100,000 and prison terms up to 5 years if the offense is committed under false pretenses • Fines up to $250,000 and prison terms up to 10 years if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

Title	Citation	Affected Stakeholders	Key Provisions
HIPAA Privacy Rule	*Standards for Privacy of Individually Identifiable Health Information; Final Rule*. 65 Fed. Reg. 82462 (December 28, 2000). Codified at 45 CFR Parts 160, and 164.	• Health care plans • Health care providers, and • Clearinghouses, as these terms are defined by the HIPAA Privacy and Security Rules	Provides individuals with many rights, including the rights to: • Request and receive copies of their health records • Request that corrections be added to their health records • Receive a notice explaining how each covered entity uses and shares health information • Decide whether to permit their information to be used or shared for certain purposes • Receive a report on when and why their health information is shared • Ask to be reached somewhere other than home • Ask covered entities to not share their information • File complaints
Medicare Improvements for Patients and Providers Act of 2008	Public Law 110-275 (Jul 15, 2008)	• Medicare recipients • Health care professionals	• To amend titles XVIII and XIX of the Social Security Act to extend expiring provisions under the Medicare Program, to improve beneficiary access to preventive and mental health services, to enhance low-income benefit programs, and to maintain access to care in rural areas, including pharmacy access, and for other purposes. • Sec. 132. Incentives for electronic prescribing • Sec. 149. Adding certain entities as originating sites for payment of telehealth services
Red Flags Rule	*Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule*, 72 Fed. Reg. 63717-63775 (November 9, 2007).	• Any “financial institution” or “creditor,” as defined by the Rule, that are “an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). Health care organizations that meet the definition of “creditors” are covered by the Rule. • Users of consumer reports • Customers of financial	• Financial institutions and creditors must develop and implement an Identity Theft Prevention Program in connection with both new and existing accounts that will prevent, detect and mitigate identity theft. • Users of consumer reports to respond to Notices of Address Discrepancies

Title	Citation	Affected Stakeholders	Key Provisions
		institutions and creditors	
State security breach notification laws	Various[135]	• Organizations conducting business in states with these statutes • Customers of organizations that are residents of states with these laws	• Requires businesses to provide notifications to state residents of breaches of their personal information • Some variance among the states on the maximum amount of time that may elapse between the breach and notification, exemptions, and liabilities • Many statutes provide individuals whose information is breached the right to sue for damages • California's state law, SB 1386, was the first and influential, and has recently been modified to cover breaches of data held by a health care provider or insurer
The Freedom of Information Act	As amended by Public Law 104-231, codified at 5 U.S.C. § 552	• Federal agencies • Any person wanting information held by the government	• A Federal agency must release any agency record unless that record falls within one of the nine statutory exemptions and three exclusions. • Covers only records in the possession and control of Federal agencies. The FOIA was amended recently by PL 104-231.
The Identity Theft and Assumption Deterrence Act of 1998	Public Law 105-318, codified at 18 U.S.C. § 47	• Federal Trade Commission (FTC) • Victims of identity theft	• Makes the FTC a central clearinghouse for identity theft complaints • Requires the FTC to: – Log and acknowledge such complaints – Provide victims with relevant information – Refer their complaints to appropriate entities (e.g., the major national consumer reporting agencies and other law enforcement agencies)
The Identity Theft Penalty Enhancement Act of 2004	Public Law 108–275, codified at 18 U.S.C. § 47	• Anyone that "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person" • Department of Justice prosecutors	Provides for increased jail time (up to 2 years) for identity thieves or those that abet identity theft
The Privacy Act of 1974	Public Law 93-579, codified in part at 5 U.S.C. § 552a	• Federal agencies • Individuals whose personal information is contained within any "system of records" held by a federal agency	• Protects records that can be retrieved by personal identifiers • Provides individuals with the right to access their own records and to request correction of these records if applicable • Prohibits disclosure of these records without written individual consent unless one of the twelve disclosure exceptions enumerated in the Act applies

[135] The National Conference of State Legislatures maintains a table of state security breach notification laws at See http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm, retrieved on September 8, 2008.